PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-216045
(43)Date of publication of application : 10.08.2001

(51)Int.Cl G06F 1/00
G06F 15/00
H04L 9/32

(21)Application number : 2000-025816
(22)Date of filing : 03.02.2000

(71)Applicant : NEC CORP
(72)Inventor : UCHIDA KAORU

(54) BIOMETRICS INPUTTING DEVICE AND BIOMETRICS COLLATING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a biometrics inputting device capable of surely verifying a person himself or herself without generating any security hole even when biometrics inputting part and processing part are not necessarily integrated.
SOLUTION: A fingerprint sensor 11 photographs a fingerprint picture when a finger is touchedand converts the photographed input picture into digital dataand transmits it to a picture enciphering part 13. The picture enciphering part 13 enciphers the input picture based on an encipherment key from an encipherment key holding part 12. A picture decoding part 21 decodes the signal received from the fingerprint inputted device 1 by using the key from the encipherment information holding part 24. A fingerprint feature extracting part 22 calculated features to be used for fingerprint collation from the picture information being the decoded result. A fingerprint feature collating part 23 collates the fingerprint features obtained by the fingerprint feature extracting part 22 with the fingerprint features of a user registered for an each user fingerprint registration information table 26and transfers the result to a collated result judging part 25.

CLAIMS

[Claim(s)]
[Claim 1]A biometrics inputting device comprising:
A sensor means which digitizes biometrics which is the living body feature peculiar to an individual.

Confidential information holding mechanism holding an enciphering key which is the confidential information set up beforehand.
A biometrics encoding means which enciphers and outputs biometrics digitized by said sensor means based on an enciphering key held at said confidential information holding mechanism.

[Claim 2]The biometrics inputting device according to claim 1 constituting said sensor meanssaid confidential information holding mechanismand said biometrics encoding means as an indivisible portion.
[Claim 3]The biometrics inputting device according to claim 1 or 2 using a fingerprint as said biometrics.
[Claim 4]A biometrics inputting device comprising:
A sensor means which digitizes biometrics which is the living body feature peculiar to an individual.
Confidential information holding mechanism holding an enciphering key which is the confidential information set up beforehand.
A digital-watermarking encoder which embeds an enciphering key held at said confidential information holding mechanism at biometrics digitized by said sensor means as digital watermarking.

[Claim 5]The biometrics inputting device according to claim 4 constituting said sensor meanssaid confidential information holding mechanismand said biometrics encoding means as an indivisible portion.
[Claim 6]The biometrics inputting device according to claim 4 or 5 using a fingerprint as said biometrics.
[Claim 7]Holding mechanism holding an enciphering key which is the confidential information beforehand set up for every biometrics inputting deviceA decoding means which decrypts the biometrics concerned using an enciphering key peculiar to said biometrics inputting device held at said holding mechanism at the time of an input of biometrics enciphered based on said enciphering keyA biometrics collating unit having a collation processing means to perform collation processing of said biometrics decrypted by said decoding means.
[Claim 8]The biometrics collating unit according to claim 7 using a fingerprint as said biometrics.
[Claim 9]A decoding means which decrypts the biometrics concerned using an enciphering key peculiar to said biometrics inputting device which came to hand separately at the time of an input of biometrics enciphered based on an enciphering key which is the confidential information beforehand set up for every biometrics inputting deviceA biometrics collating unit having a collation processing means to perform collation processing of said biometrics decrypted by said decoding means.
[Claim 10]The biometrics collating unit according to claim 9 using a fingerprint as said

biometrics.
[Claim 11]A biometrics collating unit comprising:
Holding mechanism holding an enciphering key which is the confidential information beforehand set up for every biometrics inputting device.
A means which takes out said enciphering key from the biometrics concerned at the time of an input of biometrics where said enciphering key was embedded as digital watermarking.
A means to compare said the taken-out enciphering key with an enciphering key held at said holding mechanismand to judge the justification of a signal from said biometrics inputting device.
A collation processing means to perform collation processing of said biometrics using the decision result.

[Claim 12]The biometrics collating unit according to claim 11 using a fingerprint as said biometrics.
[Claim 13]A biometrics collating unit comprising:
A means which takes out said enciphering key from the biometrics concerned at the time of an input of biometrics where an enciphering key which is the confidential information beforehand set up for every biometrics inputting device was embedded as digital watermarking.
A means to compare said the taken-out enciphering key with confidential information peculiar to said biometrics inputting device which came to hand separatelyand to judge the justification of a signal from said biometrics inputting device.
A collation processing means to perform collation processing of said biometrics using the decision result.

[Claim 14]The biometrics collating unit according to claim 13 using a fingerprint as said biometrics.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]Especially this invention relates to the biometrics inputting device and biometrics collating unit for the user authentication in an information security etc.and identification about a biometrics inputting device and a biometrics collating unit.
[0002]
[Description of the Prior Art]In the information service which leadsthe electronization and the network of information for reservation of the security which opposes the

injustice and crime of tapping and an alterationand "spoofing" of dataRealization of personal dentification for the partner of whether human being who accesses information is a user with just authorityand exchange of value to check whether you are a user whom he desires serves as indispensable conditions.
[0003]Although the magnetic card and the password are used for personal identification nowFor examplewhen a card is lost or you forget a passwordin any casethere is a problem that others become and clear up easily by a theft and forgeryor a furtive glance and a guessas well as there being inconvenient [that the person himself/herself cannot useeither].
[0004]Thenthe biometrics which solves these problems is used. The living body feature peculiar to an individual [like a fingerprint] whose biometrics is is used. It is supposed that the fingerprint which is a pattern of dermatoglyphic of human being's fingertip has the feature - "permanent throughout the life" "unique throughout the world"and since the same fingerprint is restored from the eternal dermis of the back even if epidermis receives damageit is widely known as biometrics which enables a precise individual's identification.
[0005]A "biometrics inputting device" with which the system which attests an individual by biometrics acquires fundamentally the biometrics which the user presented by the system sideThe "feature extraction part" which searches for the feature which processes the inputted data and is used for collationIt comprises "collation and a judgment part" which compares with registration data and input data (the features) the registration data ("template") about the registered user who asks beforehand and memorizesand determines whether be the same person.
[0006]The feature is similar enough as a result of collationand if judged with the presentation person of biometrics being a registered userthe authentication demand person can receive the service to demand by an authentication success. Hereaftera fingerprint is mentioned and explained as an example of biometrics.
[0007]In order to acquire an optical systemespecially a high contrast picture conventionally as an input device of a fingerprintonly the method of using the total internal reflection in prism has been used. After this applies the light emitted with the LED (Light Emitting Diode) light source to prisma photo detector like CCD (Charge Coupled Device) receives itUnevenness of the finger put on the reflector of prism is made to reflect in the difference in reflectanceand is digital-image-ized.
[0008]The unevenness is sensed in recent years as an element which makes sensing other than an optical system possible from the fingerprint which carried out direct contact on the surface of the semiconductor chipfor examplethe thing of a capacitive sensing methodthe thing of the method which detects temperature and the difference of an electric fieldetc. are being put in practical use.
[0009]
[Problem(s) to be Solved by the Invention]The method of an input device performing only the input of a fingerprint and carrying out as a realization method of fingerprint

authentication processingby the server etc. which were connected with PC (personal computer) to which identification processing was connectedor the network may be taken.
[0010]Thuswhen the fingerprint input device (scanner) and the collation processing section have dissociatedan input device (called an input scanner and an input sensor) inputs a fingerprint imageit is sent to PC through a cable etc.and feature extractionand collation and decision processing are performed there.
[0011]A cable is changedother information machines and equipment are tied with such compositionand there may be a security attack of inputting into a collation processing section the image data of others' fingerprint which came to hand at other opportunities [an input sensor]. In this casealthough the fingerprint of the person himself/herself who demands service is considered and service is permitted in a collation processing sectionit may happen that it was others' fingerprint actually.
[0012]Thenwithout producing a security holeeven when the purpose of this invention cancels the above-mentioned problem and the biometrics input part and the treating part are not necessarily unifyingIt is in providing the biometrics inputting device and biometrics collating unit which can perform positive personal identification.
[0013]
[Means for Solving the Problem]A biometrics inputting device by this invention is provided with the following.
A sensor means which digitizes biometrics which is the living body feature peculiar to an individual.
Confidential information holding mechanism holding an enciphering key which is the confidential information set up beforehand.
A biometrics encoding means which enciphers and outputs biometrics digitized by said sensor means based on an enciphering key held at said confidential information holding mechanism.

[0014]Other biometrics inputting devices by this invention are provided with the following.
A sensor means which digitizes biometrics which is the living body feature peculiar to an individual.
Confidential information holding mechanism holding an enciphering key which is the confidential information set up beforehand.
A digital-watermarking encoder which embeds an enciphering key held at said confidential information holding mechanism at biometrics digitized by said sensor means as digital watermarking.

[0015]A biometrics collating unit by this invention is provided with the following.
Holding mechanism holding an enciphering key which is the confidential information beforehand set up for every biometrics inputting device.

A decoding means which decrypts the biometrics concerned using an enciphering key peculiar to said biometrics inputting device held at said holding mechanism at the time of an input of biometrics enciphered based on said enciphering key.
A collation processing means to perform collation processing of said biometrics decrypted by said decoding means.

[0016]Other biometrics collating units by this invention are provided with the following.
A decoding means which decrypts the biometrics concerned using an enciphering key peculiar to said biometrics inputting device which came to hand separately at the time of an input of biometrics enciphered based on an enciphering key which is the confidential information beforehand set up for every biometrics inputting device.
A collation processing means to perform collation processing of said biometrics decrypted by said decoding means.

[0017]Another biometrics collating unit by this invention is provided with the following.
Holding mechanism holding an enciphering key which is the confidential information beforehand set up for every biometrics inputting device.
A means which takes out said enciphering key from the biometrics concerned at the time of an input of biometrics where said enciphering key was embedded as digital watermarking.
A means to compare said the taken-out enciphering key with an enciphering key held at said holding mechanismand to judge the justification of a signal from said biometrics inputting device.
A collation processing means to perform collation processing of said biometrics using the decision result.

[0018]Furthermore it is based on this inventionanother biometrics collating unit is provided with the following.
A means which takes out said enciphering key from the biometrics concerned at the time of an input of biometrics where an enciphering key which is the confidential information beforehand set up for every biometrics inputting device was embedded as digital watermarking.
A means to compare said the taken-out enciphering key with confidential information peculiar to said biometrics inputting device which came to hand separatelyand to judge the justification of a signal from said biometrics inputting device.
A collation processing means to perform collation processing of said biometrics using the decision result.

[0019]That isa biometrics inputting device of this invention is enciphering biometrics data acquired with an input device with a key peculiar to an input deviceor embedding data peculiar to an input device as digital watermarkingand enables a check of the

justification of a biometrics inputting device by the collating-unit side.
[0020]Since it becomes possible to detect it when a biometrics inputting device is converted and replaced by this or an output signal is replacedIt becomes possible to perform positive personal identificationwithout producing a security holeeven when a biometrics input part and a treating part are not necessarily unifying.
[0021]
[Embodiment of the Invention]Nextworking example of this invention is described with reference to Drawings. Drawing 1 is a block diagram showing the composition of the biometrics inputting device by one working example of this invention. An example of the composition in the case of logging in a user with a fingerprint in PC etc. in drawing 1 is shownthe fingerprint input device 1 is connected to PC by local connection of a cable etc.and the fingerprint collating part 2 operates by the software on PC.
[0022]The fingerprint input device 1 is equipped with the fingerprint sensor 11and when a user's finger contactsafter the fingerprint sensor 11 photos the fingerprint image and changes the photoed inputted image into digital datait is sent to the picture enciphering part 13. The enciphering key attaching part 12 holds the enciphering key peculiar to the individual of the fingerprint input device 1 as confidential information which is not known by the general user etc. This is a 256-bit bit string etc.for example.
[0023]The picture enciphering part 13 receives the enciphering key from the enciphering key attaching part 12and performs encryption processing of an inputted image by making this into a key. Although the encryption method of a common secret key method which makes DES (Data Encryption Sandard) an example can be used as this encryption processingit is also possible touse the cipher system of a public key system (asymmetric cipher system) which makes a RSA method an example on the other hand. In this casethe secret key which the fingerprint input device 1 has will be used for encryption.
[0024]The method of adopting the scramble processing shifted or replaced for every line of an inputted image or pixel depending on a use even if it is not complicated encryption processingand putting on the enciphering key attaching part 12 by using as an enciphering key the rule which specifies the scramble is also possible.
[0025]On the other handit is desirable to constitute the fingerprint sensor 11the picture enciphering part 13and the enciphering key attaching part 12 from an indivisible method as construction of the fingerprint input device 1. The unjust third party who aims at a decipherment and reconstruction of the portion here as it is indivisibleDecode the internal signal from the fingerprint sensor 11 to the picture enciphering part 13and the internal signal from the enciphering key attaching part 12 to the picture enciphering part 13orI hear that it constitutes so that those signals may be replaced by the signal from the outsidethe contents of each component may be decoded or it cannot convertand it is.
[0026]The method of burning the picture enciphering part 13 and the enciphering key

attaching part 12 is effective on the chip same as this real overseas subsidiary as the semiconductor chip which performs image acquisition of the fingerprint sensor 11and digitizatic n. As an examplethe imager chip of CMOS (Complementary Metal Oxide Semiconductor) is used as an image pick-up part of the fingerprint sensor 11There may be mounting of performing from maintenance of an encryption key to encipherment arithmetic on the same chipand making the enciphered result into an output signal.

[0027]Or fingerprint sensing of the capacitive sensing method by a semiconductor sensor can be used as a fingerprint image acquisition method of the fingerprint sensor 11and it can also be said that from maintenance of an encryption key to encipherment arithmetic is mounted on the semiconductor sensor.

[0028]In the fingerprint collating part 2 connected to the fingerprint input device 1 by local connection of a cable etc.to the encipherment information attaching part 24 of the inside. For every individual of the fingerprint input device 1 which the fingerprint collating part 2 connects and usesa peculiar enciphering key is made into the identifier (device ID) of the input deviceand a pairand is memorizedand the key corresponding to device ID of the fingerprint input device 1 which should be connected now is passed to the fingerprint decoding section 21. The image decoding part 21 decodes the signal received from the fingerprint input device 1 using the key.

[0029]it has that this decoding processing can restore the right meaningful signal using the thing corresponding to the contents of processing of the picture enciphering part 13 of the fingerprint input device 1and the justification of the signal sent from the fingerprint input device 1 and there is checked -- things -- **

[0030]For exampleif the picture enciphering part 13 uses the encryption method of the common secret key methodWhen decoding using the same key as what was held at the enciphering key attaching part 12 is performed and it can decode correctly nowit can check that the signal sent from the fingerprint input device 1 and there is just.

[0031]If it is a cipher system of a public key system (asymmetric cipher system)it will decode using the public key corresponding to the secret key held at the enciphering key attaching part 12 of the fingerprint input device 1. When it can decode correctly nowit can check that the signal sent from the fingerprint input device 1 and there is just.

[0032]The picture enciphering part 13 shifts for every line of an inputted imageor pixelorAlso when the scramble processing to replace is usedit holds to the encipherment information attaching part 24 by using as a key the rule which specifies the scramble which the enciphering key attaching part 12 should haveand decryption corresponding using it is performed. When it can decode correctly nowit can check that the signal sent from the fingerprint input device 1 and there is just.

[0033]The fingerprint feature extraction part 22 calculates the feature used for fingerprint authentication from the picture information of the result decoded by the

image decoding part 21. The fingerprint registration information table 26 classified by user holds the fingerprint feature information used for fingerprint authentication for every user. The fingerprint feature collating part 23 performs collation with the fingerprint feature searched for by the fingerprint feature extraction part 22and a user's fingerprint feature registered into the fingerprint registration information table 26 classified by userand passes a result to the collation result determining part 25.
[0034]As an example of realization of the fingerprint collation device containing the above fingerprint sensor 11the fingerprint feature appearance part 22and the fingerprint feature collating part 23there is "fingerprint collation device" indicated to JPS56-24675A or JPH4-33065A.
[0035]In the "fingerprint collation device" indicated to JPS56-24675A. The local coordinates system determined by each focus peculiar with the positions X and Y and the direction D of each focus by which a fingerprint pattern is characterized when comparing a fingerprint etc. these days in the neighborhood divided into two or more sectorial regions The ridge count of a dot and the above-mentioned focusThat isby inspecting relationhigh-precision collation is enabled stably.
[0036]In the "fingerprint collation device" indicated to JPH4-33065Ait is supposed that it participates in neither the theft of a passwordnor oblivionand that operativity is excellent and it is possible in reliable identification by performing collation with one finger or two or more fingers of alland the input fingerprint which are registered.
[0037]The collation result determining part 25 synthesizes the justification of the signal sent from the fingerprint input device 1and the result of the fingerprint authentication called for by the fingerprint feature collating part 23and outputs them as a result of personal identification. It searches for the key information which must be [that the fingerprint collating part 2 is peculiar to the fingerprint input device 1 which should be used as stated previouslyand] secret from the table of the encipherment information attaching part 24the signal sent from the fingerprint input device 1 using it is decodedand it checks whether it is the right meaningful signal.
[0038]When it means having agreed in the form of the signal outputted from the fingerprint sensor 11 in the right meaningful signal 1i.e.a fingerprint input deviceand this has agreedthe fingerprint input device 1 is justIt is judged that a fingerprint collated result is a reliable thing noting that it is able to check that the signal from the fingerprint input device 1 is not changed on the way.
[0039]Since iton the other handmeans that didn't it have the just fingerprint input device 1or the signal from the fingerprint input device 1 was changed on the way when it is not able to decode [agree] correctlyit will be judged that a fingerprint collated result is not a reliable thing.
[0040]Drawing 2 is a block diagram showing the composition of the picture input device by other working example of this invention. In drawing 2an example of the composition in the case of logging in a user with a fingerprint in PC etc. is shown like one working example of this inventionthe fingerprint input device 3 is connected to

PC by local connection of a cable etc.and the fingerprint collating part 4 operates by the software on PC.
[0041]The fingerprint input device 3 is equipped with the fingerprint sensor 11and when a user's finger contactsafter the fingerprint sensor 11 photos the fingerprint image and changes the photoed inputted image into digital datait is sent to the digital-watermarking encoder 31. The fingerprint input device confidential information attaching part 33 holds confidential information peculiar to the individual of the fingerprint input device 3 as confidential information which is not known by the general user etc. This is a character string like a passwordetc.for example.
[0042]The digital-watermarking encoder 31 receives the confidential information from the fingerprint input device confidential information attaching part 33and embeds this with a digital-watermarking encoding method at an inputted image. With electronic watermark technologyit has the following features.
[0043]. Namely(1) watermark data can be embedded in the invisible state into contents. (2) It has the feature that it is difficult for a third party to remove digital watermarkingwith the utility value of (4) contents which they can remain even if (3) watermarks which can be extracted when those who embedded the watermark are required process contentsand can be extracted maintained. (2) sets up information like the key in encoding technologyand if it does not use a keyit is performed by establishing the structure which cannot take out information.
[0044]Without degrading the fingerprint image which is contents by using the above-mentioned electronic watermark technologyelectronic watermark data can be embedded into it and the data can be kept secret. Without degrading a fingerprint image substantiallycan separate and delete watermark data and it cannot be changedeither. As an example of the real overseas subsidiary of electronic watermark technologyfor example among JPH8-241403A are the method of a descriptionart given in JPH10-2247933Aetc.
[0045]By the method of a descriptionto JPH8-241403A. Although the pixel of a watermark picture can be inspected and the contents of the picture can be clearly seen by correcting the pixel to which a current image corresponds by changing the not a chromaticity but luminosity about each of the pixel which is not the "transparence" value as which the value was specifiedHe is trying to bring about the visible mark which considers unapproved use of a picture and in which it is stopped.
[0046]With the art of a descriptionto JPH10-2247933A. Management of the electronic watermark data to insert is simplified with outputting the electronic watermark data inserted with the MPEG (Moving Picture Experta Group) stream in which digital watermarking was inserted.
[0047]As construction of the above-mentioned fingerprint input device 3it is desirable like one working example of this invention to constitute the fingerprint sensor 11the fingerprint input device confidential information attaching part 33and the digital-watermarking encoder 31 from an indivisible method. Since the output signal of the

digital-watermarking encoder 31 is included in the form in which a user's fingerprint image data appears as it isin the cryptopart 32encryption processing is performed for communication content secrecy. Cipher systemssuch as a secret common key system etc. of DES usually used oftenmay be sufficient as thisand it should just be sharing the decoding part 41 and key information which are described below.

[0048]In the fingerprint collating part 4 connected to the fingerprint input device 3 by local connection of a cable etc.in the decoding part 41the encryption for communication content secrecy is solved firstand the output signal of the digital-watermarking encoder 31 is restored. Thenin the digital-watermarking decoder 42decoding (decryption) processing corresponding to the method of encoding of the digital-watermarking encoder 31 is performedand the watermark data embedded there is separated and detected from a fingerprint image signal.

[0049]The fingerprint input device 3 sends ID (identifier) peculiar to the device to the fingerprint collating part 4 apart from a fingerprint image signal. In the fingerprint collating part 4confidential information corresponding to the individual of the fingerprint input device 3 which the fingerprint collating part 4 connects and uses for the fingerprint input device ID attaching part 43 of the inside is made into the identifier (device ID) of the input deviceand a pairand is memorized. This confidential information is the same as that of the information currently held at the fingerprint input device confidential information attaching part 33 of the applicable fingerprint input device.

[0050]The fingerprint input device ID attaching part 43 pulls this table by ID received from the fingerprint input device 3reads corresponding confidential informationand passes it to the fingerprint input device ID comparison part 44. The fingerprint input device ID comparison part 44 compares the value with the watermark data detected in the digital-watermarking decoder 42. If the fingerprint input device 3 is justthese must be in agreementotherwisewill become inharmonious.

[0051]The fingerprint feature extraction part 22 calculates the feature used for fingerprint authentication from the picture information outputted from the digital-watermarking decoder 42. The fingerprint registration information table 26 classified by user holds the fingerprint feature information used for fingerprint authentication for every user. The fingerprint feature collating part 23 performs collation with the fingerprint feature searched for by the fingerprint feature extraction part 22and the fingerprint feature registered into the fingerprint registration information table 26 classified by userand passes a result to the collation result determining part 25.

[0052]The collation result determining part 25 synthesizes the justification of the fingerprint input device 3 which the fingerprint input device ID comparison part 44 judgesand the result of the fingerprint authentication called for by the fingerprint feature collating part 23and outputs them as a result of personal identification. If the information which must be [that the fingerprint collating part 4 is peculiar to the fingerprint input device 3 which should be usedand] secret is embedded as digital

watermarking as stated previouslythe fingerprint input device 3 is justIt is judged that it is what can trust a fingerprint collated result noting that it is able to check that the signal from the fingerprint input device 3 is not changed on the way.
[0053]Since it means that didn't it have the just fingerprint input device 3or the signal from the fingerprint input device 3 was changed on the way when that is not rightit will be judged that it is not what can trust a fingerprint collated result.
[0054]Drawing 3 is a block diagram showing the composition of the picture input device by another working example of this invention. In drawing 3the picture input device by other working example of this invention is extended to the fingerprint authentication connected with the network.
[0055]The fingerprint input device 5 is connected to the service client 7 which a user uses. The POS (Point Of Sales) terminal for the public at the shop front of PC on the desk of a user's officePC at a user's homeor a storeetc. may be sufficient as this. Although these service clients work as a providing terminal of various information services or Electronic Commerce Technology Division to the user who is a customerabout the personal identification and attestation of a userit functions as a transparent fixer who mediates between communication with the fingerprint server 6 and the fingerprint input device 5 without changing contents.
[0056]The fingerprint input device 5 connected to the service client 7 has the same composition as other working example of this inventionand performs same operation. The fingerprint input picture where digital watermarking was embedded passes the service client 7and is sent to the fingerprint server 6.
[0057]The fingerprint server 6 connected to the service client 7 by the network has the same composition as other working example of this invention fundamentallyand performs same operation. That isdigital watermarking is detectedthe justification of the fingerprint input device 5 judged by this and the result of the fingerprint authentication called for by the fingerprint feature collating part 23 are synthesizedand it outputs as a result of personal identification.
[0058]Howeverunlike the case of other working example of this inventionthe public-key-encryption part 51 enciphers the confidential information held independently at the fingerprint input device confidential information attaching part 33 using the public key of the RSA method corresponding to the fingerprint server 6and a fingerprint image signal sends the fingerprint input device 5 to the fingerprint server 6.
[0059]In the secret key decoding part 61the sent signal is decoded with the secret key corresponding to its public keyand is used for comparison in the fingerprint input device ID comparison part 44. The confidential information enciphered using the public key of the RSA method corresponding to the fingerprint server 6 can be decoded only with the secret key corresponding to the public key.
[0060]Although the real overseas subsidiary that the fingerprint server 6 holds beforehand the pair of the confidential information and the fingerprint input device 5 correspor ding to all the fingerprint input devices 5 tied in the network according to

other working example of this invention about this portion to that inside is also possiblecf courseIn order for the number of the fingerprint input devices 5 to increase and to correspond to changeexchangeetc.it can be said that the direction to which confidential information is sent directly is excellent in another channel in this way.
[0061]The fingerprint server 6 tells the service client 7 about the output of the collation result determining part 25Restricting to the time when it has checked from the result of the judgmentif the user who inputted the fingerprint is a regular user and the fingerprint input device 5 is a regular devicethe service client 7 provides the service which a user demands to the user.
[0062]Although explanation of working example of above-mentioned this invention mentions and explains the case of a fingerprint as an example of biometricsIf a means to input another biometrics for the portions of the fingerprint feature extraction part 22 and the fingerprint feature collating part 23 as the fingerprint sensor 11and to extract and compare the feature replacesit is also possible to use other biometricssuch as palm printa facethe irisa vasa-sanguinea-retinae patternpalm geometrya handand a voiceprint. For examplein the case of a voiceprintthe justification of an input part can be checked by being inputted with a microphone and giving embedding of encryption or digital watermarking with a device indivisible from a microphone to Ushiro's digitized voice data.
[0063]Thusby using for communication between a biometrics inputting device and a collating unit a signal undecipherable other than a collating unitor the signal which cannot decode and change digital watermarking embedded into ita biometrics inputting device not being converted and replaced but judging that it is just -- the person himself/herself -- attestation can be performed.
[0064]A biometrics inputting device is connected with a collating unit in a cablea networketc. by thisEven when having dissociateda cable can be changedother information machines and equipment can be tiedand the security attack of the kind of inputting into a collation processing section the image data of others' fingerprint which came to hand at other opportunities [an input sensor] can be prevented. That isalthough the fingerprint of the person himself/herself who demands service is considered and service is permitted in a collation processing sectionit cannot happen that it was others' fingerprint in practice.
[0065]That iswhen are replaced with the fingerprint data from the incongruent scanner with which data is not registered and operation is added to some datayou can detect themwhen a part is lost and can make it reflected in an authentication result.
[0066]Also when many biometrics inputting devices are on a network by taking the composition of another working example of this inventionuser authentication can be realized checking that each is just.
[0067]
[Effect of the Invention]As explained aboveaccording to this inventionthe biometrics which is the living body feature peculiar to an individual is digitizedBy enciphering and

outputting the digitized biometrics based on the enciphering key which is the confidential information set up beforehandIt is effective in the ability to perform positive personal identificationwithout producing a security holeeven when the biometrics input part and the treating part are not necessarily unifying.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a block diagram showing the composition of the biometrics inputting device by one working example of this invention.
[Drawing 2]It is a block diagram showing the composition of the biometrics inputting device by other working example of this invention.
[Drawing 3]It is a block diagram showing the composition of the biometrics inputting device by another working example of this invention.
[Description of Notations]
13and 5 Fingerprint input device
2 and 4 Fingerprint collating part
6 Fingerprint server
7 Service client
11 Fingerprint sensor
12 Enciphering key attaching part
13 Picture enciphering part
21 Image decoding part
22 Fingerprint feature extraction part
23 Fingerprint feature collating part
24 Encipherment information attaching part
25 Collation result determining part
26 The fingerprint registration information table classified by user
31 Digital-watermarking encoder
32 Cryptopart
33 Fingerprint input device confidential information attaching part
41 Decoding part
42 Digital-watermarking decoder
43 Fingerprint input device ID attaching part
44 Fingerprint input device ID comparison part
51 Public-key-encryption part
61 Secret key decoding part

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－216045
（P2001－216045A）
(43)公開日　平成13年８月10日(2001.8.10)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
Ｇ０６Ｆ	1/00	３７０	Ｇ０６Ｆ 1/00	３７０Ｅ	５Ｂ０８５
	15/00	３３０	15/00	３３０Ｆ	５Ｊ１０４
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ 9/00	６７３Ｄ	

審査請求　有　　請求項の数14　ＯＬ　（全 ９ 頁）

(21)出願番号　特願2000－25816(P2000－25816)

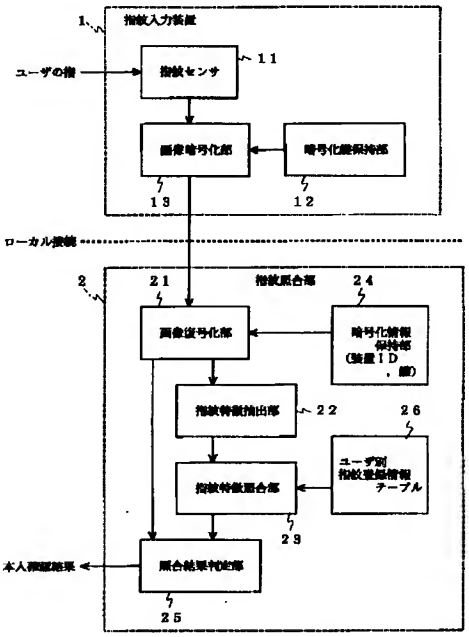
(22)出願日　平成12年２月３日(2000.2.3)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　内田　薫
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100088812
弁理士　▲柳▼川　信

Ｆターム(参考)　5B085 AE13 AE26 AE29
5J104 AA07 AA14 KA01 KA04 KA16
KA17 NA02

(54)【発明の名称】　バイオメトリクス入力装置及びバイオメトリクス照合装置

(57)【要約】
【課題】　バイオメトリクス入力部と処理部とが必ずしも一体化していない場合でもセキュリティホールを生じさせることなく、確実な本人確認を行うことが可能なバイオメトリクス入力装置を提供する。
【解決手段】　指紋センサ１１は指が接触した際にその指紋画像を撮影し、撮影した入力画像をディジタルデータに変換してから画像暗号化部１３に送る。画像暗号化部１３は暗号化鍵保持部１２から暗号化鍵を基に入力画像の暗号化処理を行う。画像復号化部２１は暗号化情報保持部２４からの鍵を用い、指紋入力装置１から受取った信号を復号する。指紋特徴抽出部２２は復号された結果の画像情報から指紋照合に用いる特徴を計算する。指紋特徴照合部２３は指紋特徴抽出部２２で求められた指紋特徴とユーザ別指紋登録情報テーブル２６に登録されているユーザの指紋特徴との照合を行い、結果を照合結果判定部２５に渡す。



【特許請求の範囲】

【請求項１】　個人に固有の生体特徴であるバイオメトリクスをディジタル化するセンサ手段と、予め設定された秘密情報である暗号化鍵を保持する秘密情報保持手段と、前記センサ手段でディジタル化されたバイオメトリクスを前記秘密情報保持手段に保持された暗号化鍵に基づいて暗号化して出力するバイオメトリクス暗号化手段とを有することを特徴とするバイオメトリクス入力装置。

【請求項２】　前記センサ手段と前記秘密情報保持手段及び前記バイオメトリクス暗号化手段とを不可分な部分として構成するようにしたことを特徴とする請求項１記載のバイオメトリクス入力装置。

【請求項３】　前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項１または請求項２記載のバイオメトリクス入力装置。

【請求項４】　個人に固有の生体特徴であるバイオメトリクスをディジタル化するセンサ手段と、予め設定された秘密情報である暗号化鍵を保持する秘密情報保持手段と、前記センサ手段でディジタル化されたバイオメトリクスに前記秘密情報保持手段に保持された暗号化鍵を電子透かしとして埋め込む電子透かしエンコーダとを有することを特徴とするバイオメトリクス入力装置。

【請求項５】　前記センサ手段と前記秘密情報保持手段及び前記バイオメトリクス暗号化手段とを不可分な部分として構成するようにしたことを特徴とする請求項４記載のバイオメトリクス入力装置。

【請求項６】　前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項４または請求項５記載のバイオメトリクス入力装置。

【請求項７】　バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵を保持する保持手段と、前記暗号化鍵に基づいて暗号化されたバイオメトリクスの入力時に前記保持手段に保持された前記バイオメトリクス入力装置固有の暗号化鍵を用いて当該バイオメトリクスを復号化する復号化手段と、前記復号化手段で復号化された前記バイオメトリクスの照合処理を行う照合処理手段とを有することを特徴とするバイオメトリクス照合装置。

【請求項８】　前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項７記載のバイオメトリクス照合装置。

【請求項９】　バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵に基づいて暗号化されたバイオメトリクスの入力時に別途入手した前記バイオメトリクス入力装置固有の暗号化鍵を用いて当該バイオメトリクスを復号化する復号化手段と、前記復号化手段で復号化された前記バイオメトリクスの照合処理を行う照合処理手段とを有することを特徴とするバイオメトリクス照合装置。

【請求項１０】　前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項９記載のバイオメトリクス照合装置。

【請求項１１】　バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵を保持する保持手段と、前記暗号化鍵が電子透かしとして埋め込まれたバイオメトリクスの入力時に当該バイオメトリクスから前記暗号化鍵を取り出す手段と、その取り出された前記暗号化鍵と前記保持手段に保持された暗号化鍵とを比較して前記バイオメトリクス入力装置からの信号の正当性を判定する手段と、その判定結果を用いて前記バイオメトリクスの照合処理を行う照合処理手段とを有することを特徴とするバイオメトリクス照合装置。

【請求項１２】　前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項１１記載のバイオメトリクス照合装置。

【請求項１３】　バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵が電子透かしとして埋め込まれたバイオメトリクスの入力時に当該バイオメトリクスから前記暗号化鍵を取り出す手段と、その取り出された前記暗号化鍵と別途入手した前記バイオメトリクス入力装置固有の秘密情報とを比較して前記バイオメトリクス入力装置からの信号の正当性を判定する手段と、その判定結果を用いて前記バイオメトリクスの照合処理を行う照合処理手段とを有することを特徴とするバイオメトリクス照合装置。

【請求項１４】　前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項１３記載のバイオメトリクス照合装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はバイオメトリクス入力装置及びバイオメトリクス照合装置に関し、特に情報セキュリティ等におけるユーザ確認、個人識別のためのバイオメトリクス入力装置及びバイオメトリクス照合装置に関する。

【０００２】

【従来の技術】情報の電子化やネットワークを通じての情報サービスにおいて、データの盗聴・改竄や「なりすまし」といった不正・犯罪に対抗するセキュリティの確保のためには、情報にアクセスする人間が正当な権限を持つユーザであるか、または価値の交換の相手が自分の望むユーザであるかを確認するための本人確認の実現が必須の条件となる。

【０００３】現在、本人確認には磁気カードやパスワードが利用されているが、例えばカードをなくしたり、パスワードを忘れてしまうと本人でも使えないという不便さがあるのはもちろん、いずれの場合も盗難・偽造や盗み見・推量によって容易に他人がなりすませるという問題点がある。

【０００４】そこで、これらの問題点を解決するバイオメトリクスが用いられる。バイオメトリクスとは指紋のような個人に特有な生体特徴を利用するものである。人間の指先の皮膚紋様である指紋は「万人不同」・「終生不変」という特徴を持つとされ、表皮が損傷を受けてもその奥の不変な真皮から同じ指紋が復元されるため、精密な個人の同定を可能にするバイオメトリクスとして広く知られている。

【０００５】バイオメトリクスによって個人を認証するシステムは基本的に、ユーザが提示したバイオメトリクスをシステム側で取得する「バイオメトリクス入力装置」と、入力されたデータを処理し照合に用いる特徴を求める「特徴抽出部」と、予め求めて記憶しておく正規ユーザについての登録データ（「テンプレート」）と、登録データと入力データ（の特徴同士）とを比較して同一人物であるか否かを決定する「照合・判定部」とから構成されている。

【０００６】照合の結果、特徴が十分類似し、バイオメトリクスの提示者が登録ユーザであると判定されれば、認証成功ということで、認証要求者は要求するサービスを受けられる。以下、バイオメトリクスの例として指紋を挙げて説明する。

【０００７】指紋の入力装置としては従来、光学方式、特に高コントラストな画像を得るためにプリズムでの全反射を利用する方法のみが用いられてきている。これはＬＥＤ（Ｌｉｇｈｔ　Ｅｍｉｔｔｉｎｇ　Ｄｉｏｄｅ）光源で発した光をプリズムに当ててからＣＣＤ（Ｃｈａｒｇｅ　Ｃｏｕｐｌｅｄ　Ｄｅｖｉｃｅ）のような受光素子で受け、プリズムの反射面に置いた指の凹凸を反射率の違いに反映させ、ディジタル画像化するというものである。

【０００８】また近年は、光学方式以外のセンシングを可能とする素子として、半導体チップの表面に直接接触させた指紋からその凹凸をセンスする、例えば静電容量方式のもの、温度や電界の差を検知する方式のもの等も実用化されつつある。

【０００９】

【発明が解決しようとする課題】指紋照合処理の実現方法としては、入力装置が指紋の入力だけを行い、識別処理が接続されたＰＣ（パーソナルコンピュータ）やネットワークで結ばれたサーバ等で行うという方法がとられることがある。

【００１０】このように、指紋入力装置（スキャナ）と照合処理部とが分離している場合、入力装置（入力スキャナ、入力センサと呼ばれることもある）は指紋画像の入力を行い、それをケーブル等を通してＰＣに送り、そこで特徴抽出や照合・判定処理が実行される。

【００１１】このような構成ではケーブルを付け替えて他の情報機器を結び、他の機会に入手した他人の指紋の画像データを、入力センサを装って照合処理部に入力するというセキュリティアタックがあり得る。この場合、照合処理部ではサービスを要求する本人の指紋と考えてサービスを許可するが、実際には他人の指紋であったということが起こりうる。

【００１２】そこで、本発明の目的は上記の問題点を解消し、バイオメトリクス入力部と処理部とが必ずしも一体化していない場合でもセキュリティホールを生じさせることなく、確実な本人確認を行うことができるバイオメトリクス入力装置及びバイオメトリクス照合装置を提供することにある。

【００１３】

【課題を解決するための手段】本発明によるバイオメトリクス入力装置は、個人に固有の生体特徴であるバイオメトリクスをディジタル化するセンサ手段と、予め設定された秘密情報である暗号化鍵を保持する秘密情報保持手段と、前記センサ手段でディジタル化されたバイオメトリクスを前記秘密情報保持手段に保持された暗号化鍵に基づいて暗号化して出力するバイオメトリクス暗号化手段とを備えている。

【００１４】本発明による他のバイオメトリクス入力装置は、個人に固有の生体特徴であるバイオメトリクスをディジタル化するセンサ手段と、予め設定された秘密情報である暗号化鍵を保持する秘密情報保持手段と、前記センサ手段でディジタル化されたバイオメトリクスに前記秘密情報保持手段に保持された暗号化鍵を電子透かしとして埋め込む電子透かしエンコーダとを備えている。

【００１５】本発明によるバイオメトリクス照合装置は、バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵を保持する保持手段と、前記暗号化鍵に基づいて暗号化されたバイオメトリクスの入力時に前記保持手段に保持された前記バイオメトリクス入力装置固有の暗号化鍵を用いて当該バイオメトリクスを復号化する復号化手段と、前記復号化手段で復号化された前記バイオメトリクスの照合処理を行う照合処理手段とを備えている。

【００１６】本発明による他のバイオメトリクス照合装置は、バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵に基づいて暗号化されたバイオメトリクスの入力時に別途入手した前記バイオメトリクス入力装置固有の暗号化鍵を用いて当該バイオメトリクスを復号化する復号化手段と、前記復号化手段で復号化された前記バイオメトリクスの照合処理を行う照合処理手段とを備えている。

【００１７】本発明による別のバイオメトリクス照合装置は、バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵を保持する保持手段と、前記暗号化鍵が電子透かしとして埋め込まれたバイオメトリクスの入力時に当該バイオメトリクスから前記暗号化鍵を取り出す手段と、その取り出された前記暗号化鍵と前記保持手段に保持された暗号化鍵とを比較して前記バイオメ

トリクス入力装置からの信号の正当性を判定する手段と、その判定結果を用いて前記バイオメトリクスの照合処理を行う照合処理手段とを備えている。

【００１８】本発明によるさらに別のバイオメトリクス照合装置は、バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵が電子透かしとして埋め込まれたバイオメトリクスの入力時に当該バイオメトリクスから前記暗号化鍵を取り出す手段と、その取り出された前記暗号化鍵と別途入手した前記バイオメトリクス入力装置固有の秘密情報とを比較して前記バイオメトリクス入力装置からの信号の正当性を判定する手段と、その判定結果を用いて前記バイオメトリクスの照合処理を行う照合処理手段とを備えている。

【００１９】すなわち、本発明のバイオメトリクス入力装置は、入力装置で取得されるバイオメトリクスデータを入力装置固有の鍵で暗号化し、あるいは入力装置固有のデータを電子透かしとして埋め込むことで、照合装置側でバイオメトリクス入力装置の正当性を確認可能とする。

【００２０】これによって、バイオメトリクス入力装置が改造・置換され、あるいは出力信号が置換された場合にそれを検知することが可能となるので、バイオメトリクス入力部と処理部とが必ずしも一体化していない場合でもセキュリティホールを生じさせることなく、確実な本人確認を行うことが可能となる。

【００２１】

【発明の実施の形態】次に、本発明の実施例について図面を参照して説明する。図１は本発明の一実施例によるバイオメトリクス入力装置の構成を示すブロック図である。図１においてはＰＣ等においてユーザのログインを指紋で行う場合の構成の一例を示しており、指紋入力装置１をケーブル等のローカルな接続によってＰＣに接続し、ＰＣ上のソフトウェアで指紋照合部２が動作するようになっている。

【００２２】指紋入力装置１には指紋センサ１１が装備されており、指紋センサ１１はユーザの指が接触した際にその指紋画像を撮影し、撮影した入力画像をディジタルデータに変換してから画像暗号化部１３に送る。暗号化鍵保持部１２は一般ユーザ等に知られていない秘密情報としてその指紋入力装置１の個体固有の暗号化鍵を保持する。これは、例えば２５６ビットのビット列等である。

【００２３】画像暗号化部１３は暗号化鍵保持部１２からその暗号化鍵を受取り、これを鍵として入力画像の暗号化処理を行う。この暗号化処理としては、ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓａｎｄａｒｄ）を例とするような共通秘密鍵方式の暗号化方法を用いることができるが、また一方、ＲＳＡ方式を例とするような公開鍵方式（非対称暗号系）の暗号化方式を利用することも可能である。この場合、指紋入力装置１の持つ秘密鍵を暗号化に用いることになる。

【００２４】また、用途によっては複雑な暗号化処理でなくても、入力画像のラインや画素毎にシフトしたり、入れ替えたりするスクランブル処理を採用し、そのスクランブルを規定するルールを暗号化鍵として暗号化鍵保持部１２に置くという方法も可能である。

【００２５】一方、指紋入力装置１の構成法としては、指紋センサ１１、画像暗号化部１３、暗号化鍵保持部１２を不可分な方法で構成することが望ましい。不可分であるとは、ここの部分の解読や改造を図る不当な第三者が、指紋センサ１１から画像暗号化部１３への内部信号、暗号化鍵保持部１２から画像暗号化部１３への内部信号を解読したり、それらの信号を外部からの信号で置き換えたり、あるいはそれぞれの構成要素の中身を解読したり改造したりできないように構成するということである。

【００２６】この実現法としては、指紋センサ１１の画像取得及びディジタル化を実行する半導体チップと同一チップ上に画像暗号化部１３と暗号化鍵保持部１２とを焼き込むという方法が有効である。一例としては、指紋センサ１１の撮像部としてＣＭＯＳ（Ｃｏｍｐｌｅｍｅｎｔａｒｙ　Ｍｅｔａｌ　Ｏｘｉｄｅ　Ｓｅｍｉｃｏｎｄｕｃｔｏｒ）のイメージャチップを利用し、その同一チップ上で暗号鍵の保持から暗号化演算までを行い、暗号化した結果を出力信号とするという実装があり得る。

【００２７】あるいは、指紋センサ１１の指紋画像取得方法として半導体センサによる静電容量方式の指紋センシングを利用し、その半導体センサ上に暗号鍵の保持から暗号化演算までを実装するということもできる。

【００２８】指紋入力装置１とケーブル等のローカルな接続によって結ばれた指紋照合部２ではその内部の暗号化情報保持部２４に、その指紋照合部２が接続して使用する指紋入力装置１の個体毎に固有な暗号化鍵を、その入力装置の識別子（装置ＩＤ）と対にして記憶しておき、現在接続されているはずの指紋入力装置１の装置ＩＤに対応する鍵を指紋復号化部２１に渡す。画像復号化部２１はその鍵を用い、指紋入力装置１から受取った信号を復号する。

【００２９】この復号処理は指紋入力装置１の画像暗号化部１３の処理内容に対応したものを用い、正しく意味ある信号が復元できることをもって、指紋入力装置１及びそこから送られてくる信号の正当性を確認することなる。

【００３０】例えば、画像暗号化部１３が共通秘密鍵方式の暗号化方法を用いていれば、暗号化鍵保持部１２に保持されたものと同一の鍵を用いた復号を行い、これで正しく復号できる場合には指紋入力装置１及びそこから送られてくる信号が正当なものであることを確認することができる。

【００３１】また、公開鍵方式（非対称暗号系）の暗号

化方式であれば、指紋入力装置１の暗号化鍵保持部１２に保持された秘密鍵に対応する公開鍵を用いて復号する。これで正しく復号できる場合には指紋入力装置１及びそこから送られてくる信号が正当なものであることを確認することができる。

【００３２】さらに、画像暗号化部１３が入力画像のラインや画素毎にシフトしたり、入れ替えたりするスクランブル処理を用いた場合にも、暗号化鍵保持部１２が持っているはずのスクランブルを規定するルールを鍵として暗号化情報保持部２４に保持しておき、それを用いて対応する復号化を行う。これで正しく復号できる場合には指紋入力装置１及びそこから送られてくる信号が正当なものであることを確認することができる。

【００３３】指紋特徴抽出部２２は画像復号化部２１で復号された結果の画像情報から指紋照合に用いる特徴を計算する。ユーザ別指紋登録情報テーブル２６は指紋照合に用いる指紋特徴情報をユーザ毎に保持している。指紋特徴照合部２３は指紋特徴抽出部２２で求められた指紋特徴とユーザ別指紋登録情報テーブル２６に登録されているユーザの指紋特徴との照合を行い、結果を照合結果判定部２５に渡す。

【００３４】以上の指紋センサ１１、指紋特徴出部２２、指紋特徴照合部２３を含む指紋照合装置の実現例としては、特開昭５６－２４６７５号公報や特開平４－３３０６５号公報に記載された「指紋照合装置」がある。

【００３５】特開昭５６－２４６７５号公報に記載された「指紋照合装置」では、指紋等の照合に際して、指紋紋様を特徴付ける各特徴点の位置Ｘ，Ｙ及び方向Ｄとともに各特徴点により固有に決定される局所座標系を複数個の扇形領域に分割した近傍における最近傍点と上記特徴点との隆線数、すなわちリレーションを検査することによって、安定で、かつ精度の高い照合を可能にしている。

【００３６】また、特開平４－３３０６５号公報に記載された「指紋照合装置」では、登録されている一つの指もしくは複数の指の全てと入力指紋との照合を行うことによって、暗証番号の盗難や忘却に関与しない、操作性が優れかつ信頼性の高い同定を可能としている。

【００３７】照合結果判定部２５は指紋入力装置１から送られてくる信号の正当性と、指紋特徴照合部２３で求められる指紋照合の結果とを総合し、本人確認の結果として出力する。先に述べたように、指紋照合部２は使用されているはずの指紋入力装置１に固有で秘密であるはずの鍵情報を暗号化情報保持部２４のテーブルから探索し、それを用いて指紋入力装置１から送られる信号を復号し、それが正しく意味ある信号であるか否かを確認する。

【００３８】正しく意味ある信号とはすなわち、指紋入力装置１において指紋センサ１１から出力された信号の形式に合致していることを意味し、これが合致している場合には指紋入力装置１が正当なもので、また指紋入力装置１からの信号は途中で改変されていないことが確認できたとして、指紋照合結果は信頼できるものであると判断する。

【００３９】一方、合致していない等、正しく復号できなかった場合には、それは指紋入力装置１が正当なものではないか、または指紋入力装置１からの信号が途中で改変されたことを意味するので、指紋照合結果は信頼できるものではないと判断することになる。

【００４０】図２は本発明の他の実施例による画像入力装置の構成を示すブロック図である。図２においては本発明の一実施例と同様に、ＰＣ等においてユーザのログインを指紋で行う場合の構成の一例を示しており、指紋入力装置３をケーブル等のローカルな接続によってＰＣに接続し、ＰＣ上のソフトウェアで指紋照合部４が動作する。

【００４１】指紋入力装置３には指紋センサ１１が装備されており、指紋センサ１１はユーザの指が接触した際にその指紋画像を撮影し、撮影した入力画像をディジタルデータに変換してから電子透かしエンコーダ３１に送る。指紋入力装置秘密情報保持部３３は一般ユーザ等に知られていない秘密情報としてその指紋入力装置３の個体固有の秘密情報を保持する。これは、例えばパスワードのような文字列等である。

【００４２】電子透かしエンコーダ３１は指紋入力装置秘密情報保持部３３からその秘密情報を受取り、電子透かしエンコード方式によってこれを入力画像に埋め込む。電子透かし技術とは次のような特徴を持つ。

【００４３】すなわち、（１）透かしデータをコンテンツの中に、不可視の状態で埋め込むことができる、（２）透かしを埋め込んだ者が必要な時に抽出することが可能である、（３）透かしはコンテンツを加工しても残り、抽出が可能である、（４）コンテンツの利用価値を保ったまま第三者が電子透かしを除去するのは困難であるという特徴を持つ。（２）は暗号化技術におけるキーのような情報を設定し、キーを用いなければ情報が取り出せないような仕組みを設けることによって行われる。

【００４４】上記の電子透かし技術を使用することによって、コンテンツである指紋画像を劣化させることなく、電子透かしデータをその中に埋め込むことができ、そのデータを秘密に保つことができる。また、指紋画像を大幅に劣化させることなく、透かしデータを分離・削除・改変することもできない。電子透かし技術の実現法の例としては、例えば特開平８－２４１４０３号公報に記載の方法や特開平１０－２２４７９３３号公報に記載の技術等がある。

【００４５】特開平８－２４１４０３号公報に記載の方法では、ウォーターマーク画像の画素を検査し、その値が指定された「透明」値でない画素のそれぞれについ

て、現画像の対応する画素を、その色度ではなく輝度を変更することによって修正することで、画像の内容を明瞭に見ることができるが、画像の無認可使用をおもいとどまらせる可視のマークをもたらすようにしている。

【００４６】また、特開平１０－２２４７９３３号公報に記載の技術では、電子透かしが挿入されたＭＰＥＧ（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔａ　Ｇｒｏｕｐ）ストリームとともに、挿入された電子透かしデータも出力することで、挿入する電子透かしデータの管理を簡単にしている。

【００４７】尚、上記の指紋入力装置３の構成法としては、本発明の一実施例と同様に、指紋センサ１１、指紋入力装置秘密情報保持部３３、電子透かしエンコーダ３１を不可分な方法で構成することが望ましい。また、電子透かしエンコーダ３１の出力信号はこのままユーザの指紋画像データが見える形で含むので、通信内容秘匿のために暗号部３２において暗号化処理を行う。これは通常よく使われるＤＥＳの秘密共通鍵方式等の暗号化方式でよく、以下に述べる復号部４１と鍵情報を共用していればよい。

【００４８】指紋入力装置３とケーブル等のローカルな接続によって結ばれた指紋照合部４においては、まず復号部４１において通信内容秘匿のための暗号化を解き、電子透かしエンコーダ３１の出力信号を復元する。その後、電子透かしデコーダ４２において、電子透かしエンコーダ３１のエンコードの方法に対応したデコード（復号化）処理を行い、指紋画像信号からそこに埋め込まれた透かしデータを分離して検出する。

【００４９】指紋入力装置３は指紋画像信号とは別に、その装置固有のＩＤ（識別子）を指紋照合部４に送る。指紋照合部４ではその内部の指紋入力装置ＩＤ保持部４３に、その指紋照合部４が接続して使用する指紋入力装置３の個体に対応する秘密情報をその入力装置の識別子（装置ＩＤ）と対にして記憶しておく。この秘密情報は該当指紋入力装置の指紋入力装置秘密情報保持部３３に保持されている情報と同一のものである。

【００５０】指紋入力装置ＩＤ保持部４３は指紋入力装置３から受取ったＩＤでこのテーブルをひき、対応する秘密情報を読出して指紋入力装置ＩＤ比較部４４に渡す。指紋入力装置ＩＤ比較部４４はその値と、電子透かしデコーダ４２において検出された透かしデータとを比較する。もしも、指紋入力装置３が正当なものであればこれらは一致するはずであり、そうでなければ不一致となる。

【００５１】指紋特徴抽出部２２は電子透かしデコーダ４２から出力された画像情報から指紋照合に用いる特徴を計算する。ユーザ別指紋登録情報テーブル２６は指紋照合に用いる指紋特徴情報をユーザ毎に保持しているものである。指紋特徴照合部２３は指紋特徴抽出部２２で求められた指紋特徴とユーザ別指紋登録情報テーブル２６に登録された指紋特徴との照合を行い、結果を照合結果判定部２５に渡す。

【００５２】照合結果判定部２５は指紋入力装置ＩＤ比較部４４が判定する指紋入力装置３の正当性と、指紋特徴照合部２３で求められる指紋照合の結果とを総合し、本人確認の結果として出力する。先に述べたように、指紋照合部４は使用されているはずの指紋入力装置３に固有で秘密であるはずの情報が電子透かしとして埋め込まれていれば、指紋入力装置３が正当なもので、また指紋入力装置３からの信号が途中で改変されていないことを確認することができたとして、指紋照合結果を信頼できるものであると判断する。

【００５３】そうでない場合には、それは指紋入力装置３が正当なものではないか、または指紋入力装置３からの信号が途中で改変されたことを意味するので、指紋照合結果を信頼できるものではないと判断することになる。

【００５４】図３は本発明の別の実施例による画像入力装置の構成を示すブロック図である。図３においては本発明の他の実施例による画像入力装置をネットワークで結ばれた指紋照合に拡張したものである。

【００５５】指紋入力装置５はユーザが利用するサービスクライアント７に接続されている。これは例えばユーザのオフィスの机の上にあるＰＣ、ユーザの家庭にあるＰＣ、あるいは店舗の店頭等にある公衆向けのＰＯＳ（Ｐｏｉｎｔ　Ｏｆ　Ｓａｌｅｓ）端末でもよい。これらのサービスクライアントは顧客であるユーザに対してさまざまな情報サービスや電子商取引の提供端末として働くが、ユーザの本人確認・認証に関しては指紋サーバ６と指紋入力装置５との通信を、中身を変えずに橋渡しする透明な仲介者として機能する。

【００５６】サービスクライアント７に接続された指紋入力装置５は本発明の他の実施例と同様の構成を持ち、同様の動作を行う。電子透かしが埋め込まれた指紋入力画像はサービスクライアント７を通過して指紋サーバ６に送られる。

【００５７】サービスクライアント７とネットワークによって結ばれた指紋サーバ６は基本的に本発明の他の実施例と同様の構成を持ち、同様の動作を行う。すなわち、電子透かしを検出し、これによって判定される指紋入力装置５の正当性と、指紋特徴照合部２３で求められる指紋照合の結果とを総合し、本人確認の結果として出力する。

【００５８】但し、指紋入力装置５は、本発明の他の実施例の場合と異なり、指紋画像信号とは別に指紋入力装置秘密情報保持部３３に保持された秘密情報を、公開鍵暗号部５１が指紋サーバ６に対応するＲＳＡ方式の公開鍵を用いて暗号化して指紋サーバ６に送る。

【００５９】秘密鍵復号部６１では送られてきた信号を自分の公開鍵に対応した秘密鍵によって復号し、指紋入

力装置ＩＤ比較部４４での比較に用いる。指紋サーバ６に対応するＲＳＡ方式の公開鍵を用いて暗号化された秘密情報は、その公開鍵に対応した秘密鍵によってのみ復号可能である。

【００６０】この部分については本発明の他の実施例に準じて、ネットワーク内に結ばれた全ての指紋入力装置５に対応する秘密情報と指紋入力装置５との対を予め指紋サーバ６がその内部に保持しておくという実現法ももちろん可能ではあるが、指紋入力装置５の数が多くなり、また変更・交換等に対応するためには、このように別のチャネルで直接秘密情報を送る方が優れているといえる。

【００６１】指紋サーバ６は照合結果判定部２５の出力をサービスクライアント７に知らせ、指紋を入力したユーザが正規のユーザでありかつ指紋入力装置５が正規の装置であると判定の結果から確認できた時に限り、サービスクライアント７はユーザの要求するサービスをそのユーザに対して提供する。

【００６２】上記の本発明の実施例の説明では、バイオメトリクスの一例として指紋の場合を挙げて説明しているが、指紋センサ１１と、指紋特徴抽出部２２、指紋特徴照合部２３の部分を別のバイオメトリクスを入力し、特徴を抽出して照合する手段で置換すれば、掌紋、顔、虹彩、網膜血管パターン、掌形、筆跡、声紋等の他のバイオメトリクスを使用することも可能である。例えば、声紋の場合にはマイクで入力され、ディジタル化された後の音声データに対してマイクと不可分な装置で暗号化や電子透かしの埋め込みを施すことで、入力部の正当性を確認することができる。

【００６３】このように、照合装置以外は解読できない信号、あるいはその中に埋め込まれた電子透かしを解読し、また改変できない信号をバイオメトリクス入力装置と照合装置との間での通信に用いることによって、バイオメトリクス入力装置が改造、置換されず正当なものであることを判定して本人認証を実行することができる。

【００６４】これによって、バイオメトリクス入力装置が照合装置とケーブルやネットワーク等で接続され、分離している場合でも、ケーブルを付け替えて他の情報機器を結び、他の機会に入手した他人の指紋の画像データを、入力センサを装って照合処理部に入力するという種類のセキュリティアタックを防ぐことができる。つまり、照合処理部ではサービスを要求する本人の指紋と考えてサービスを許可するが、実際は他人の指紋であったということは起こり得ない。

【００６５】すなわち、データが登録されていない不適合スキャナからの指紋データで置き換えられた場合、データの一部に操作が加えられた場合、一部が失われた場合にはそれらを検知し、認証結果に反映させることができる。

【００６６】また、本発明の別の実施例の構成をとることによって、ネットワーク上に多数のバイオメトリクス入力装置がある場合にも、それぞれが正当なものであることを確認しながらユーザ認証を実現することができる。

【００６７】

【発明の効果】以上説明したように本発明によれば、個人に固有の生体特徴であるバイオメトリクスをディジタル化し、そのディジタル化したバイオメトリクスを予め設定された秘密情報である暗号化鍵に基づいて暗号化して出力することによって、バイオメトリクス入力部と処理部とが必ずしも一体化していない場合でもセキュリティホールを生じさせることなく、確実な本人確認を行うことができるという効果がある。

【図面の簡単な説明】

【図１】本発明の一実施例によるバイオメトリクス入力装置の構成を示すブロック図である。

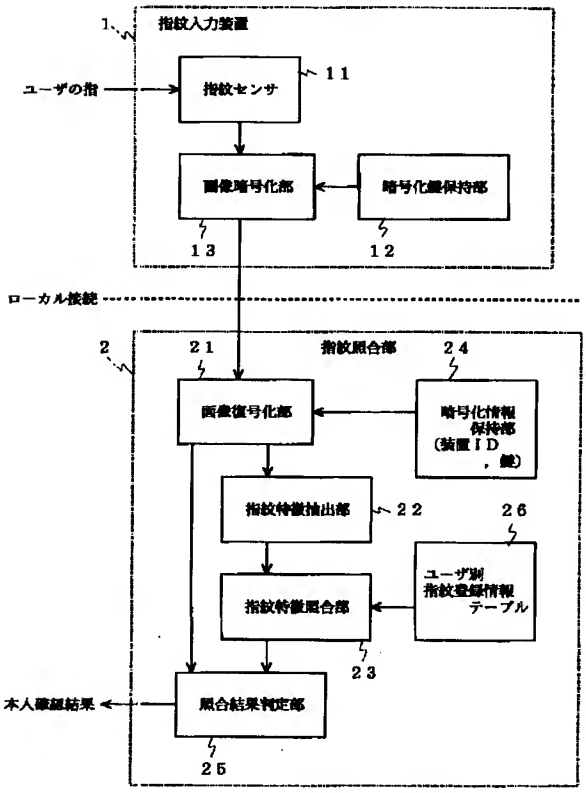
【図２】本発明の他の実施例によるバイオメトリクス入力装置の構成を示すブロック図である。

【図３】本発明の別の実施例によるバイオメトリクス入力装置の構成を示すブロック図である。

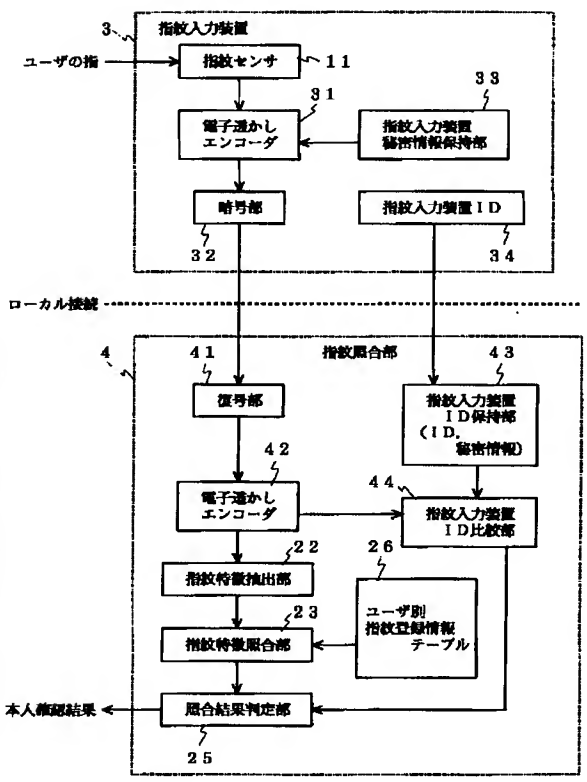
【符号の説明】

１，３，５　指紋入力装置
２，４　指紋照合部
６　指紋サーバ
７　サービスクライアント
１１　指紋センサ
１２　暗号化鍵保持部
１３　画像暗号化部
２１　画像復号化部
２２　指紋特徴抽出部
２３　指紋特徴照合部
２４　暗号化情報保持部
２５　照合結果判定部
２６　ユーザ別指紋登録情報テーブル
３１　電子透かしエンコーダ
３２　暗号部
３３　指紋入力装置秘密情報保持部
４１　復号部
４２　電子透かしデコーダ
４３　指紋入力装置ＩＤ保持部
４４　指紋入力装置ＩＤ比較部
５１　公開鍵暗号部
６１　秘密鍵復号部

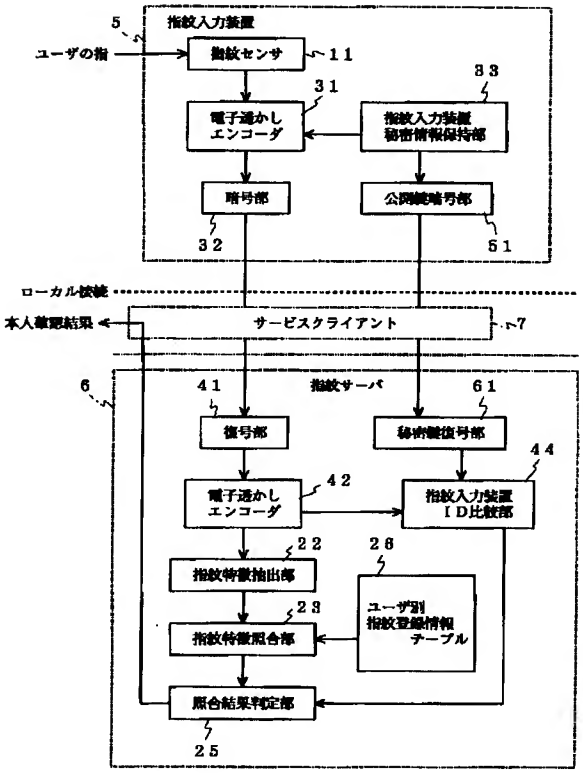
【図１】


1
指紋入力装置
ユーザの指
指紋センサ
11
画像暗号化部
暗号化鍵保持部
13
12
ローカル接続
2
21
指紋照合部
24
画像復号化部
暗号化情報保持部（装置ＩＤ，鍵）
指紋特徴抽出部
22
26
ユーザ別指紋登録情報テーブル
指紋特徴照合部
23
本人確認結果
照合結果判定部
25

【図２】


3
指紋入力装置
ユーザの指
指紋センサ
11
31
33
電子透かしエンコーダ
指紋入力装置秘密情報保持部
暗号部
指紋入力装置ＩＤ
32
34
ローカル接続
4
41
指紋照合部
43
復号部
指紋入力装置ＩＤ保持部（ＩＤ，秘密情報）
42
44
電子透かしエンコーダ
指紋入力装置ＩＤ比較部
22
26
指紋特徴抽出部
ユーザ別指紋登録情報テーブル
23
指紋特徴照合部
本人確認結果
照合結果判定部
25

【図３】


5
指紋入力装置
ユーザの指
指紋センサ
11
31
33
電子透かし
エンコーダ
指紋入力装置
秘密情報保持部
暗号部
公開鍵暗号部
32
51
ローカル接続
本人確認結果
サービスクライアント
7
6
41
指紋サーバ
61
復号部
秘密鍵復号部
44
42
電子透かし
エンコーダ
指紋入力装置
ＩＤ比較部
22
26
指紋特徴抽出部
ユーザ別
指紋登録情報
テーブル
23
指紋特徴照合部
照合結果判定部
25